REMARKS

Claims 1, 14-20, 22-32, and 34 are pending in this application.

Applicants have amended claims 1, 27, 30, and 32. The changes to these claims made herein do not introduce any new matter.

Rejection under 35 U.S.C. § 101

In response to the rejection of claims 1, 14-20, 22-26, 32, and 34 under 35 U.S.C. § 101 as being directed toward non-statutory subject matter, Applicants have amended independent claims 1 and 32. In particular, Applicants have amended claim 1 to specify that each operation of the method for protected execution of a cryptographic calculation is executed by an integrated circuit. Applicants have amended claim 32 to specify that the portable data carrier includes a processor and a storage, with the storage having a computer program stored thereon, and the computer program including program commands to cause the processor to execute the method for protected execution of a cryptographic calculation.

Accordingly, Applicants submit that claims 1, 14-20, 22-26, 32, and 34 now define statutory subject matter under 35 U.S.C. § 101, and request that the rejection of these claims thereunder be withdrawn.

Rejection Under 35 U.S.C. § 103

Applicants respectfully request reconsideration of the rejection of claims 1, 14-20, 22-32, and 34 under 35 U.S.C. § 103(a) as being unpatentable over *Walmsley et al.* ("*Walmsley*") (US 2003/0159036 A1, which corresponds to WO 01/61918 A1) in view of *Ngo et al.* ("*Ngo*") (US 2003/0097628 A1) and *Boneh et al.* ("*Boneh*") (US 6,965,673 B1). As will be explained in more detail below, the combination of *Walmsley* of in view of *Ngo* and *Boneh* would not have rendered the subject matter defined in independent claims 1, 27, 30, and 32, as amended herein, obvious to one having ordinary skill in the art.

In support of the obviousness rejection, the Examiner asserts that Paragraphs [0628], [0629], and [0652], and [0657] of *Walmsley* disclose the following features specified in present claim 1 (see the Final Office Action at page 4):

> wherein an integrity check of the key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter.

In addition, the Examiner considers that the random number R (see Paragraph [0628]) and the memory vector M (see Paragraph [0629]) correspond to the two key parameters specified in present claim 1 (see the Final Office Action at page 10).

Applicants respectfully traverse the Examiner's characterization of the *Walmsley* reference relative to the presently claimed subject matter. In particular, Applicants respectfully traverse the Examiner's characterization of the *Walmsley* reference relative to the recitation of "a key with at least two key parameters." Neither the random number R nor the memory vector M relied upon by the Examiner is a parameter of "a key with at least two key parameters," as specified in the claimed subject matter. On page 10 of the Final Office Action, the Examiner states that "*a parameter is any factor that helps define a system* it does not necessarily mean it forms the overall key." [Emphasis added.] Consequently, the Examiner considers a key parameter to be any factor that helps define a key. However, neither R nor M helps to define a key. To the contrary, R and M are totally independent from any keys.

Moreover, even if, for the sake of discussion, R and M were to be considered as the two claimed key parameters, the cited portions of the *Walmsley* reference do not disclose (or suggest) the features of the claimed subject matter. The Examiner appears to be asserting that the claimed integrity check corresponds to the verification of the property $E_{KA}[R|M] = R|M$, which is disclosed in Paragraph [0652]. However, Applicants do not understand how this verification might possibly prevent a cryptographic attack in which conclusions are drawn as

to at least one second key parameter (i.e., M or R) by corrupting at least one first key parameter (i.e., R or M). The *Walmsley* reference does not disclose any possible attack in which a conclusion is drawn as to either one of M and R, let alone an attack in which this conclusion is drawn by corrupting the other one of M and R. In Paragraph [0657], *Walmsley* states that intense testing of ChipT will reveal nothing about K_A. However, the "intense testing" is not a corruption of at least one first key parameter (i.e., R or M), and the fact that nothing is revealed about K_A does not imply any conclusion as to at least one second key parameter (i.e., M or R).

Furthermore, even if the keys K_T (see Paragraph [0626]) and K_A (see Paragraph [0627]) were to be regarded as the two key parameters, the *Walmsley* reference still would not disclose the above-noted features of the claimed subject matter. First, this would be contrary to the claimed feature of "a key with at least two key parameters" since K_T and K_A clearly form two different keys and thus cannot be considered as key parameters of a key. Second, the cited paragraphs of *Walmsley* do not disclose any integrity check of the key. Third, even if some operation of *Walmsley* were to be regarded as an integrity check, this would be an integrity check that is performed for reasons other than *to prevent* the cryptographic attack, as specified in the claimed subject matter.

In view of the foregoing, Applicants respectfully submit that the Examiner has not identified elements in the *Walmsley* reference that could reasonably be equated to the key parameters of the claimed subject matter and also satisfy the additional features specified in claim 1. In this regard, Applicants note that it is not sufficient for the Examiner to show that 1) *Walmsley* performs an integrity check of a key, and 2) *Walmsley* prevents a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter. In addition, the Examiner would need to show that the integrity check is done *so as to prevent* the cryptographic attack recited in claim 1. An integrity check

that serves an entirely different purpose (e.g., an integrity check that prevents another kind of cryptographic attack and that is not used to prevent the cryptographic attack recited in claim 1) would not be sufficient to establish that *Walmsley* discloses the features of claim 1.

The discussion set forth above applies to both the former and the currently amended versions of claim 1. As amended herein, claim 1 further specifies that "the key is a private key for use in an RSA method and each key parameter is contained in the private key." This feature further distinguishes the claimed subject matter from the applied references. The only private key that is disclosed in *Walmsley* in connection with protocol C2 is the key K_A (see Paragraph [0627]). However, *Walmsley* does not teach that this is a private key for use in an RSA method, as claimed. Furthermore, *Walmsley* does not disclose any key parameters of this key K_A, let alone any of the other features of claim 1 regarding such key parameters. In particular, it is apparent that the elements R and M discussed above cannot reasonably be called a "key parameter contained in a private key" (i.e., private key K_A), as specified in the presently claimed subject matter.

For the reasons set forth above, the *Walmsley* reference does not teach or suggest the feature of claim 1 that "an integrity check of the key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter."

The above-noted deficiency of the *Walmsley* reference relative to the subject matter defined in present claim 1 is not cured by either the *Ngo* or *Boneh* references. The *Ngo* reference discloses a CRC checksum analysis technique, but does not contain any teaching related to the technical field of cryptography. Consequently, *Ngo* does not disclose any cryptographic calculation, let alone any key or any key parameter. Furthermore, *Ngo* does not disclose that the key parameter is the product of a value required for the cryptographic

calculation and a safeguard value, as specified in the claimed subject matter (see, for example, claim 26).

Turning to the *Boneh* reference, this reference does not cure above-noted deficiency of the *Walmsley* reference relative to the subject matter defined in present claim 1 for at least two reasons. First, the *Boneh* reference does not teach (or suggest) to perform an integrity check of the key. Second, the *Boneh* reference does not teach (or suggest) to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter (see the Amendment filed on September 29, 2008 for more detailed comments regarding the *Boneh* reference).

In summary, even if one having ordinary skill in the art were to combine the *Walmsley*, *Ngo*, and *Boneh* references in the manner proposed by the Examiner, this combination would not have resulted in each and every feature of the subject matter defined in present claim 1 due to the above-discussed deficiencies of the *Walmsley* reference relative to the claimed subject matter. As such, the combination of *Walmsley* in view of *Ngo* and *Boneh* would not have rendered the subject matter the subject matter defined in present claim 1 obvious to one having ordinary skill in the art.

Each of independent claims 27, 30, and 32, as amended herein, includes features that are substantially the same as or correspond to the above-discussed features of present claim 1. Thus, the arguments set forth above regarding present claim 1 also apply to present claims 27, 30, and 32.

Accordingly, independent claims 1, 27, 30, and 32, as amended herein, are patentable under 35 U.S.C. § 103(a) over *Walmsley* in view of *Ngo* and *Boneh*. Claims 14-20 and 22-26, each of which ultimately depends from claim 1, claims 28 and 29, each of which depends from claim 27, claim 31, which depends from claim 30, and claim 34, which depends from claim 32, are likewise patentable under 35 U.S.C. § 103(a) over *Walmsley* in view of *Ngo* and

Boneh for at least the same reasons set forth above with regard to the applicable independent claim.

Conclusion

In view of the foregoing, Applicants respectfully request reconsideration and reexamination of claims 1, 14-20, 22-32, and 34, as amended herein, and submit that these claims are in condition for allowance. Accordingly, a notice of allowance is respectfully requested. In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at **(408) 749-6902**. If any additional fees are due in connection with the filing of this paper, then the Commissioner is authorized to charge such fees to Deposit Account No. 50-0805 (Order No. WACHP006).

Respectfully submitted,
MARTINE PENILLA & GENCARELLA, L.L.P.

/Peter B. Martine/

Peter B. Martine
Reg. No. 32,043

710 Lakeway Drive, Suite 200
Sunnyvale, California 94085
Customer Number 25920